I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Applying International Environmental Legal Norms to Cyber Statecraft

JASON HEALEY AND HANNAH PITTS*

I. INTRODUCTION†

As globalization intensifies, technology creates new opportunities and challenges for states, industry, and individuals. Cyberspace is a telling example of this phenomenon; it has changed the lives of billions of people and has increased connectivity and efficiency, but cyberspace has also made individuals and governments more vulnerable to security threats, theft, and other methods of attack. Even as cyberspace has interconnected governments and people, cyber attacks can create national security threats against states and private critical infrastructure, a phenomenon that implicates the roles and responsibilities established in international policy and international law.

While international law has been successful in creating regimes to govern other aspects of interstate relations and international security, its application to cyber policy is relatively nascent. Policymakers and theorists have posited a variety of existing policy and legal frameworks to apply to the issues of cyberspace. States thus far have largely chosen to address these challenges through three approaches: technical, crime, and warfare. Each of these traditional approaches has helped,

---

* Jason Healey is the Director of the Cyber Statecraft Initiative at the Atlantic Council and is a founding board member of the Cyber Conflict Studies Association. Hannah Pitts is Executive Director of the Cyber Conflict Studies Association and Program Controller at Defense Group Inc.'s Center for Intelligence Research and Analysis.

† The authors wish to dedicate this article to Dr. Christopher C. Joyner, a respected Georgetown University professor, devoted Hoyas fan, and beloved mentor whose passion for international environmental law inspired this article. Dr. J. and his love of international law are greatly missed.

though none—singularly or collectively—has gotten the upper hand against the challenges of cyber threats.

Accordingly, it is time to look to newer approaches, such as borrowing from public health or irregular warfare. This paper will briefly review these other approaches, but focus on another often overlooked, but potentially beneficial, framework—that of applying international environmental law to the security challenges of cyberspace. This framework cannot replace those of the traditional models; that is, it will not invent more secure technologies, defeat cyber criminals, or help militaries understand the laws of armed conflict in cyberspace. However, applying environmental legal norms to cyberspace could be useful because much of international environmental law addresses a problem familiar to cyber policymakers, the inherent tension between a state's sovereignty and its obligations to individuals, other states, and a shared common space. As nations analyze their environmental rights and responsibilities under international law, they will find many concepts helpfully applicable to cyberspace as well.

II. APPROACHES FOR INTERNATIONAL CYBER SECURITY, CONFLICT, AND COOPERATION

To address cyber challenges, nation-states have tended, whether formally or informally, to use a mix of three approaches—the Technical Approach, Criminal Approach, and Warfare Approach.[1] Each is good at solving a range of problems, though each has also been unsuccessfully tried outside of that range.

Practitioners of the Technical Approach see each problem as a technical challenge to be overcome; if cyberspace is unsecured and is a hotbed of crime, we should invent new devices, standards, or methods, and respond quickly and effectively to disruptive cyber incidents. These engineers, entrepreneurs, scientists, and programmers[2] have, of course, been wildly successful at building and

---

[1] See Gregory J. Rattray & Jason Healey, Ctr. for a New Am. Sec., Non-State Actors and Cyber Conflict, in 2 AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 65 (Kristin M. Lord & Travis Sharp eds., 2011), for a deeper discussion of these approaches. The forthcoming work from the Cyber Conflict Studies Association also addresses these approaches and compares them with alternative models. More information about the work is available at www.cyberconflict.org.

[2] Key organizations that provide invaluable service to the Internet community include the Internet Engineering Task Force, International Center for Assigned Names and Numbers, The Internet Society, North American Network Operators Group, Forum of Incident Response and Security Teams, and many more.

expanding cyberspace and providing us ever more amazing capabilities, but they have not yet been able to give the defense in cyberspace any edge over hackers, organized crime, and other attackers.

The Criminal Approach entails formal legal regimes and strong, widely understood domestic and international norms for reducing crime and bringing criminals to justice. At the international level, nations share long-standing traditions by which they cooperate toward these ends. Despite these frameworks, it remains very difficult to solve cyber crimes due to a variety of problems including jurisdictional complexity; a lack of trained police, prosecutors, and judges; and problems with digital forensics and evidence.[3]

The Warfare Approach seeks to develop and apply military doctrine for threat deterrence and response. The idea has been problematic, given that few, if any, of the malicious incidents popularly called "cyber warfare" live up to such a label. A wide range of crimes, from patriot hacking[4] to WikiLeaks hacktivists,[5] have improperly been called "war," as has Chinese espionage.[6] Yet, national defense establishments continue to develop both offensive and defensive cyber capabilities[7] and there are several efforts to apply existing international law governing military matters, such as from the United Nations Charter and Geneva Conventions.[8]

---

[3] One group investigating cyber-crime found that "living in St. Petersburg, Russia, the Koobface gang might as well be living on Mars, so poorly developed are the mechanisms of international law enforcement cooperation." NART VILLENEUVE, INFORMATION WARFARE MONITOR, KOOBFACE: INSIDE A CRIMEWARE NETWORK II (2010), *available at* http://www.infowar-monitor.net/reports/iwm-koobface.pdf.

[4] *See, e.g.*, Ellen Messmer, *Kosovo Cyberwar Intensifies Chinese Hackers Targeting U.S. Sites, Government Says*, CNN, May 12, 1999, http://articles.cnn.com/1999-05-12/tech/9905_12_cyberwar.idg_1_hackers-web-servers-web-sites?_s=PM:TECH.

[5] Michael Evans & Giles Whittell, *Cyberwar Declared as China Hunts for the West's Intelligence Secrets*, THE TIMES, Mar. 8, 2010, http://technology.timesonline.co.uk/tol/news/tech_and_web/article7053254.ece.

[6] *Id.*

[7] Most notably the stand-up of U.S. Cyber Command in 2010, but other countries are also developing such capabilities, including United Kingdom, China, Germany, and France.

[8] *See, e.g.*, THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT (2000); David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87 (2010); Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121 (2009); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM.

Each of these approaches has significant advantages and their proponents are correct to drive towards new solutions. Yet twenty years of pursuing such solutions has not yet definitively changed the landscape and cyber threats are as worrisome as ever. Accordingly, it is time to look for other approaches. Three possible new approaches are to use perspectives from irregular warfare, public health, and environmental law. The first two have been introduced in other papers,[9] so this work will focus on the last, namely, how environmental laws can help address problems in cyberspace.

III. INTERNATIONAL LAW AS APPLICABLE TO TRADITIONAL CYBER SECURITY APPROACHES

To frame the discussion of the applicability of international environmental law to cyberspace, this paper will first examine the international legal constructs behind the three traditional approaches mentioned above, Technical, Criminal, and Warfare.

There is, strictly speaking, little or no international "law" that governs the Technical Approach. To the extent the Technical Approach is shaped by global norms, they emanate from a system of governance comprising a set of multi-stakeholder organizations, including the Internet Society (ISOC), Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), and the World Wide Web Consortium (W3C). While these forms of governance are foundational to the operation of cyberspace, they do not represent a comprehensive approach to securing cyberspace and influencing behavior in cyberspace.

These multi-stakeholder organizations reflect the initial ethos of the Internet pioneers and are sufficient for their current tasks. However, these forms of information international governance are unlikely to address the most pressing cyber security threats in isolation. They are crucial to the operation of cyberspace and any

---

J.TRANSNAT'L L. 885 (1999); and Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, 84 INT'L REV. RED CROSS 365 (2002). Additionally, the EastWest Institute has been pursuing this line of dialogue with a panel of United States and Russian experts, most notably KARL FREDERICK RAUSCHER & ANDREY KOROTKOV, EASTWEST INST., WORKING TOWARDS RULES FOR GOVERNING CYBER CONFLICT: RENDERING THE GENEVA AND HAGUE CONVENTIONS IN CYBERSPACE (Jan. 2011) and EASTWEST INST., RUSSIA-U.S. BILATERAL ON CYBERSECURITY: CRITICAL TERMINOLOGY FOUNDATIONS (Karl Frederick Rauscher & Valery Yaschenko eds., Apr. 2011).

[9] Rattray & Healey, *supra* note 1, at 68; *see also* the forthcoming monograph from Cyber Conflict Studies Association.

viable solutions must include these organizations, but more must be done. The multi-stakeholder organizations may be able to harden the underlying architecture or make more robust the technical framework, but these organizations cannot provide a comprehensive solution alone.

Under the Criminal Approach, international norms for cyber crime are relatively advanced, as this has been a focus of many governments, especially the United States. The U.S. focus on international norms to combat cyber crime can be clearly seen in two recent U.S. strategies, as well as its continued and strident support of the Council of Europe Convention on Cybercrime. The *International Strategy for Cyberspace* establishes as an existing international norm: "States must identify and prosecute cybercriminals, to ensure laws and practices deny criminals safe havens, and cooperate with international criminal investigations in a timely manner."[10] The more recent *Strategy to Combat Transnational Organized Crime* also views international legal and policy coordination as crucial to addressing cyber-crime: "Internationally, [the United States] will further international norms against tolerating or sponsoring crime in all its forms, including in cyberspace."[11] These strategies combined with U.S. action in organizations like Interpol and the Financial Action Task Force, demonstrate current international norms about cyber crime.

International organizations and documents have also reflected these norms. For example, "[t]he [United Nations] General Assembly has called upon states . . . to prevent their territories from being used as safe havens . . . . [and] cooperate in the investigation and prosecution of international cyber attacks."[12] The landmark cyber crime treaty, the *Council of Europe Convention on Cybercrime*, also

---

[10] THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 10 (May 2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE]. The same strategy commits the United States to participate in "international cybercrime policy development," "harmonize cybercrime laws internationally," "focus cybercrime laws on combating illegal activities, not restricting access to the Internet," and denying "terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks." *Id.* at 19–20.

[11] THE WHITE HOUSE, STRATEGY TO COMBAT TRANSNATIONAL ORGANIZED CRIME: ADDRESSING CONVERGING THREATS TO NATIONAL SECURITY 14 (July 2011), *available at* http://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf.

[12] Graham, *supra* note 8, at 94.

known as the Budapest *Convention*, expansively covers "any crimes for which it is necessary to collect evidence 'in electronic form.'"[13] The convention not only commits national governments to make illegal a range of cyber crimes (such as illegal access, interception, data or system interference, computer forgery and fraud, and child pornography),[14] but also mandates signatories to enact new procedural provisions, such as on extradition and mutual assistance.[15] Despite the development of the treaty in the *Council of Europe*, the U.S. was crucial in its creation[16] and has made the accession of non-European countries to the Convention a priority.[17]

However, the *Convention* has two main drawbacks. Over thirty nations have both signed and ratified the *Convention*, but worldwide adoption is unlikely as many nations see it as a specifically "European" document.[18] Moreover, according to Robert Knake, "Though the convention has helped develop an international standard for

---

[13] *See* Michael Vatis' excellent explanation of the treaty and its implications, The Council of Europe Convention on Cybercrime, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 207, 208 (2010).

[14]Convention on Cybercrime, Council of Europe, art. 2, Nov. 23, 2001, *available at* http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

[15] *Id.* at titles. 2, 3.

[16] See Vatis, *supra* note 13, for a discussion of U.S. actions and interests in the creation of this document.

[17] For example, the International Strategy for Cyberspace included a commitment to "harmonize cybercrime laws internationally by expanding accession to the Budapest Convention." INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 10, at 20. Further,

> The Budapest Convention on Cybercrime provides countries with a model for drafting and updating their current laws . . . . The United States will continue to encourage other countries to become parties to the Convention and will help current non-parties use the Convention as a basis for their own laws, easing bilateral cooperation in the short term, and preparing them for the possibility of accession to the Convention in the long term.

Id.

[18] ROBERT K. KNAKE, COUNCIL ON FOREIGN REL., INTERNET GOVERNANCE IN AN AGE OF CYBER INSECURITY 17 (2010). This feeling persists as only a small number of non-European countries (including the United States, Canada, Japan, and South Africa) have signed the Convention.

criminalizing cyber crime, it has not led to an appreciable reduction in cyber crime." Indeed, "Members of the convention include some of the worst cyber-criminal havens in eastern Europe . . . ."[19] This contrasts sharply with the current U.S. push for expanded accession to the *Convention*. These problems are also compounded by the practical difficulties of prosecuting cyber-crime, which is often resource-intensive and technically challenging to obtain the evidence needed for convictions.

Lastly, the Warfare Approach presents two key questions at the focus of current legal debate: whether a cyber attack could constitute a use of force under Article 2(4) of the U.N. Charter and whether a cyber attack could cross the second threshold of an "armed attack" under Article 51, which recognizes the inherent right to collective and individual self-defense.[20] Answering these questions is made difficult by the lack of a definition for "use of force" or "armed attack," but these are not new issues and they have been previously addressed in the "kinetic" context. The right to resort to force, also known as *jus ad bellum*, is articulated in Articles 2(4), 39, and 51 of the U.N. Charter. Many U.S. legal scholars and practitioners have concluded that for a cyber attack to be considered an armed attack it must have the same scope, duration, and intensity of a kinetic attack, using the traditional framework of Jean Pictet in the commentaries to the Geneva Convention.[21] That is, the effects of a cyber attack must be the same or comparable to what would be an armed attack using conventional force. The real debate, therefore, will depend on the facts of any particular attack and whether it is legally and politically accepted as an armed attack. If it is, then the victim state retains the same rights under Article 51 as in any armed attack context.

---

[19] *Id.*

[20] "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." U.N. Charter art. 2, para. 4. *See* Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825 (2001); Schmitt, *supra* note 8.

[21] For a discussion of the Pictet factors and other issues of laws of armed conflict, see Matthew J. Sklerov, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201 MIL. L. REV. 1 (2009). Jean Pictet, Vice President of the International Committee of the Red Cross, was an international humanitarian law expert, the main author of the commentary of the four Geneva Conventions of 1949, and a collaborator on the commentary for the Additional Protocols of 1977.

The second aspect of the laws of armed conflict must be briefly noted as well. *Jus in bello* principles govern uses of force whether in an armed conflict or any other context.[22] Four main principles guide *jus in bello*: military necessity, distinction or discrimination, proportionality, and humanity.[23] While these elements of jus *in bello* are elements of customary international law, the norms are also codified in the *Additional Protocol I to the 1949 Geneva Conventions*.[24] It then follows that if a state chooses to use a cyber attack in self-defense, it must comport with both *jus ad* bellum and *jus in bello principles*. The application of the laws of war dictate that any use of cyber force must fall within the parameters of these principles and that states have the same rights and responsibilities as they have in a kinetic conflict scenario.

The applicability and scope of applicability of the laws of armed conflict may still be debated in academic circles, but the United States has stated in multiple contexts its intentions in responding to significant cyber attacks. Most plainly, Deputy Secretary of Defense William J. Lynn stated in a speech unveiling the *Department of Defense Strategy for Operating in Cyberspace*, "[T]he United States reserves the right, under the laws of armed conflict, to respond to serious cyber attacks with a proportional and justified military response at the time and place of our choosing."[25] In its *International*

---

[22] For example, self-defense in response to an armed attack, while not necessarily part of an armed conflict, must comport with all laws of war, including jus in *bello* principles. *See* common Article 2 of the 1949 Geneva Conventions; Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 2, Aug. 12, 1949, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, art. 2, Aug. 12, 1949, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War, art. 2, Aug. 12, 1949, 75 U.N.T.S. 135; and Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 2, Aug. 12, 1949, 75 U.N.T.S. 287.

[23] Graham, *supra* note 8, at 98. For an in-depth exploration of this issue, see also NAT'L ACAD. OF SCI., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens et al. eds., 2009).

[24] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), Dec. 12, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

[25] William J. Lynn, III, U.S. Deputy Sec'y of Def., Remarks on the Department of Defense Cyber Strategy 10 (July 14, 2011), *available at* http://www.defense.gov/speeches/speech.aspx?speechid=1593. In addition, the Department of Defense Strategy for Operating in Cyberspace reiterates, "The Department will work with interagency and international partners to . . . reserve the right to defend these vital national assets as necessary and appropriate." U.S. DEP'T OF DEF., DEPARTMENT

Strategy for Cyberspace, the United States stated in equally unequivocal terms:

> All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.[26]

The United States, arguably the leader in many respects of international cyberspace policy, has demonstrated its commitment to operating within the laws of war when addressing cyber threats.

Basics of Environmental Norms and Cyber

1. ILC on State Responsibility: States could be held responsible for cyber activities through action or omission that are attributable to them and are a breach of an international obligation
2. Good Neighborliness: States might have an obligation to limit activities adversely affecting the territory or interests of other states through cyberspace
3. Trail Smelter Decision: States can be liable for harm from cross-border emissions, which might include botnet attacks
4. Principle 21 of Stockholm Declaration: States have sovereign use of their own resources, but a responsibility to not cause damage outside that jurisdiction, which might apply to cyberspace
5. Corfu Channel Decision: When states are aware of activities that will harm other states, they are obliged to prevent them, which could apply to botnets and other malicious attacks

---

OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 10 (July 2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf.

[26] INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 10, at 14.

The three approaches discussed above and the relevant international law, norms, and regimes have their benefits and drawbacks, as discussed above. However, they have proven, both in isolation and in concert, to be insufficient to meet the challenges of cyberspace. Accordingly, we should pursue alternative models for viewing cyberspace and its problems. Cyberspace and its challenges are not entirely new and we should therefore not reinvent the wheel. In fact, we may be able to apply the lessons and principles of other regimes and frameworks to combat the threats in cyberspace.

A. BASICS OF ENVIRONMENTAL NORMS AND CYBER

Public international law is dedicated in part to navigating the pervasive tension between the principle of state sovereignty and the scope of mutual obligations among states. In the development of international environmental law, that tension has been significantly addressed through the articulation of limited state liability for certain acts that originate within the territory of one state that cause harm to another state or to its citizens. For this reason, international environmental law offers rich possibilities for principles to help resolve the tension between sovereignty and mutual obligation in cyberspace, as noted in the text box. International environmental principles may provide significant help to delineate state responsibility for state and non-state actions.

Additionally, by viewing cyberspace as an ecosystem and applying international environmental concepts, this approach avoids some of the most sensationalized language and perspectives on cyber conflict and cyber security, allowing for more progress in developing norms and rules around cyberspace. Security and freedom (or privacy) are often reduced to a black-and-white, zero-sum discussion about two competing public goods. A new approach that shifts the debate with new language and a new paradigm might make it easier to find new consensus.

When investigating the role of environmental law for cyberspace, it is vitally important to distinguish between cyber security directed at stopping or mitigating malicious activity (such as stealing online personal information or disrupting websites) and government efforts to control information and content, which are priorities for nations like Russia and China.[27] State responsibility for policing international

[27] NATO Parliamentary Assembly, 074 CDS 11 E – Information and National Security, Draft General Report by Lord Jopling, General Rapporteur, ¶ 59 (2011). For a discussion of the respective Chinese and Russian perspectives on cyber security and information security, see also Christopher A. Ford, *The Trouble with Cyber Arms Control*, 29 NEW

content clearly conflicts with Article 19 of the *Universal Declaration of Human Rights*: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[28] However, there is far more leeway to use environmental norms for national responsibility without compromising Article 19. Accordingly, this latter meaning, to fight incorrect or unpleasant information content, is not a focus of this article, which instead looks at activities like botnets, patriotic hacking, and malicious activities even rising to the level of Stuxnet worm.

Other than cooperating to hunt down cyber criminals, there has been little international action to control the transboundary flow of malicious activities. As with the classic tragedy of the commons, there is a flawed policy that "favors pollution,"[29] which considers malicious activity to be someone else's problem, favoring inaction and allowing the malicious activity to continue. The environmental model is particularly strong at addressing these kinds of problems, where a general "dirtiness" of the environment passively allows cross-border "emissions."

In this case, the emissions are not tied directly to any specific attack, but can be treated as a general problem of pollution. For example, the United States, although the nation most targeted by denial of service attacks, is also the top country of origin for global attacks, accounting for 22% of the total.[30] Major telecommunication providers feel little pressure not to pass "polluted" cyber attack traffic downstream; according to a survey by Arbor Networks, 27% of network operators do not attempt to detect outbound or cross-bound attacks and, of those who do, nearly half take no actions to mitigate

---

ATLANTIS 52 (2010). The Russian and Chinese position is perhaps most clearly made in the Shanghai Cooperation Organization's delineation of "Major International Information Security Threats," including, "[d]issemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States." *See* Shanghai Cooperation Organization, Agreement Between the Governments of the Member States of the SCO in the Field of International Information Security, art. 2 (2008).

[28] Universal Declaration of Human Rights, G.A. Res. 217A (III), at art. 19, U.N. Doc. A/810 (Dec. 10, 1948).

[29] Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243, 1245 (Dec. 13, 1968), *available at* http://www.sciencemag.org/cgi/content/full/162/3859/1243.

[30] SYMANTEC CORP., INTERNET SECURITY THREAT REPORT VOLUME 16 (2011).

such attacks.[31] Internet Service Providers then could be seen as originating or passing along pollution by not cracking down on botnets (computers compromised and under automated control of hackers) in their networks and not filtering the attacks out of their traffic flow. Nations could be seen collectively as passively allowing the ISPs to pass along this pollution by not having sufficiently strong laws or regulations.

Another kind of activity that might be governed by the norms and principles of international environmental law are *specific* large-scale attacks, rather than the general high-level of pollution mentioned above. Here, a nation has a far more active responsibility for the attacks coming from its citizens or from within its borders.

The best example of this kind of attack is the cyber disruptions in Estonia in 2007.[32] Following the removal of a statue in Tallinn dedicated to the Soviet victory in April 2007, protests by mostly ethnic-Russians against the removal of the statue turned violent and began to spill over to cyberspace. On April 27, Estonian news websites and government websites were defaced and hit by coordinated Distributed Denial of Service (DDoS) attacks. The attacks then expanded to multiple waves of malicious activity aimed at different sectors of Estonian government and society. Because of the high level of connectivity and prevalence of e-commerce and e-government services, the DDoS attacks affected many sectors of Estonian society, including government ministries, most news organizations, banks, and communications firms.[33] While some in Nashi, a Russian youth political organization aligned with the ruling party in Russia, claimed responsibility, it is still not clear which individuals were responsible or the level of involvement of the Russian state. What is clear is the nationalist and political motivations behind the cyber attacks.

Though Technical, Criminal, and Warfare Approaches may be helpful in this case, it is possible the norms of environmental law

---

[31] ARBOR NETWORKS, WORLDWIDE INFRASTRUCTURE SECURITY REPORT VOLUME VI 15–16 (2010).

[32] For a comprehensive discussion of the Estonian case, see ENEKEN TIKK ET AL., NATO COOP. CYBER DEF. CTR. OF EXCELLENCE (2010). According to the Defense Minister at the time, "This was the first time that a botnet threatened the national security of an entire nation." Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED, Aug. 21, 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

[33] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN, May 17, 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

would provide additional avenues of pressure on Russia to prevent future attacks. Moreover, according to the Estonian government, there was attack traffic coming from 178 different countries, all of which may have had some responsibility to limit the hazardous cyber-"emissions" from their respective networks (as discussed in the previous example).[34]

This kind of "transboundary harm," seemingly originating in part from Russia, flooded Estonian networks and significantly compromised Estonian governmental and financial services for weeks. The kind of activity seen in Estonia, below the threshold of the laws of armed conflict, but sufficiently disruptive to an entire country, is potentially the most relevant for these environmental norms.

B. NORMS OF INTERNATIONAL ENVIRONMENTAL LAW

This section evaluates the potential application of norms about state responsibility for non-state actors and for transboundary harm, focusing primarily on those norms that developed as part of international environmental law. Some of these norms are not explicitly environmental in scope, but instead build a case that a nation can be held responsible for malicious cyber actions coming from within their national boundaries. As these have already been applied in environmental contexts, they illuminate the possible paths.

The section first discusses the contours of the International Law Commission's work on state responsibility before discussing environmental principles in particular. We then turn to the principle of good neighborliness, the *Corfu Channel* case, and *the Trail Smelter* arbitration, ending with Principle 21 of the *Stockholm Declaration*. The scope, enforceability, remedy, and potential cyberspace equivalent of these norms and principles are discussed in turn.

1. THE WORK OF THE INTERNATIONAL LAW COMMISSION ON STATE RESPONSIBILITY

In 2001, after many decades of work and revision, the International Law Commission (ILC) finally adopted its *Draft Articles on the Responsibility of States for Internationally Wrongful Acts* (*ILC Draft Articles*). While not binding international law, the work of the International Law Commission is important for the future of international law as "private codification," furthering the development

---

[34] Tikk, et al., *supra* note 32.

of international law.[35] Further, in December 2001, the United Nations General Assembly recognized the *ILC Draft Articles* "without prejudice to the question of their future adoption or other appropriate action."[36] *The ILC Draft Articles* mostly consider the responsibility of states for state action and do not clarify primary obligations of states. That is, the *ILC Draft Articles* as established do not seek to list all primary obligations, which includes, among other rules, "the asserted international standard of treatment and the right of diplomatic protection."[37] Instead of listing all possible violations of primary obligations, the document addresses the secondary obligations out of those violations. Although the *ILC Draft Articles* would pertain most directly to state action in cyberspace, they could have an important indirect impact on the actions of non-state actors as well.

Article 1 of the *ILC Draft Articles* states, "Every internationally wrongful act of a State entails the international responsibility of that State."[38] As elaborated in the *Commentary for the Draft Articles*, "Whether there has been an internationally wrongful act depends, first, on the requirements of the obligation which is said to have been breached, and secondly on the framework conditions for such an act . . . ."[39] The *ILC Draft Articles*, therefore, do not address what would constitute a primary obligation of a state, nor do they define in detail how to remedy the breach. That is, the *ILC Draft Articles* elucidate the

---

[35] *Introduction: Origin and Background of the Development and Codification of International Law*, INT'L LAW COMM'N, http://untreaty.un.org/ilc/ilcintro.htm (last visited Apr. 6, 2012). Experts on the ILC are elected by the United Nations General Assembly and then research international legal questions requested by the General Assembly, governments, or outside organizations. *See* Statute of the International Law Commission, G.A. Res. 174 (II) (Nov. 21, 1947), amended by G.A. Res. 485 (V) (Dec. 12, 1950); G.A. Res. 984 (X) (Dec. 3,1955); G.A. Res. 985 (X) (Dec. 3, 1955); and G.A. Res. 36/39 (Nov. 18, 1981).

[36] G.A. Res. 56/83, ¶ 3, U.N. Doc. A/RES/56/83 (Jan. 28, 2002).

[37] Daniel Bodansky & John R. Crook, *Symposium: The ILC's State Responsibility Articles: Introduction and Overview*, 96 AM. J. INT'L L. 773, 776 (2002) (citing CLYDE EAGLETON, THE RESPONSIBILITY OF STATES IN INTERNATIONAL LAW (1928)).

[38] Report of the International Law Commission on the Work of Its Fifty-third Session, UN GAOR, 56th Sess., Supp. No. 10, UN Doc. A/56/10 (2001); Draft Articles on Responsibility of States for International Wrongful Acts, with Commentaries, art. 1, [2001] 2 Y.B. Int'l Law Comm'n, 20, 32, U.N. Doc. A/CN.4/SER.A/2001 /Add. 1 (Part 2), *available at* http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [hereinafter Draft Articles on Responsibility of States for International Wrongful Acts].

[39] *Id.* art. 1, cmt. 1, at 32.

secondary obligations when a breach has occurred, but do not address what actions would constitute a breach.

An internationally wrongful act of a state can be an action or omission that, "(a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State."[40] Therefore, "it is not necessary that a state intentionally or maliciously violat[e] an international obligation to attribute responsibility."[41] A violation could conceivably encompass a state passively allowing certain activities. The scope of state responsibility thus depends on the legality of the action in question, not necessarily the degree of the harm inflicted. For example, in international environmental law, if a certain kind of pollution has severe consequences, but does not constitute a violation of a primary obligation, the state cannot be held responsible.[42] This is a significant limitation, especially when one considers extending the discussed principles to cyberspace.

The scope of the *ILC Draft Articles* is generally limited to state actions, thus falling in the traditional conception of state-dominated international politics and security. It is important to note that the *ILC Draft Articles* were adopted shortly before the terrorist attacks of September 11, 2001, the aftermath of which has affected the perspective of how relationships between state and non-state actors are viewed.[43] Still, while the *ILC Draft Articles* do not fully address the issue of non-state actors, some articles do bear relevance on the issue. Generally, it is considered that "the only conduct attributed to the State at the international level is that of its organs of government, or of others who have acted under the direction, instigation or control of those organs . . . ."[44] The ILC *Draft Articles* go on to enumerate what

---

[40] *Id.* art. 2, at 34.

[41] Alexandre Kiss, *State Responsibility and Liability for Nuclear Damage*, 35 DENV. J. INT'L L. & POL'Y 67, 78 (2008).

[42] One alternative is to create Draft Articles on "International Liability for Injurious Consequences Arising out of Acts not Prohibited by International Law." See, e.g., ELLI LOUKA, INTERNATIONAL ENVIRONMENTAL LAW: FAIRNESS, EFFECTIVENESS, AND WORLD ORDER 468 (2006).

[43] For a fuller discussion of state responsibility for non-state actors after the terrorist attacks of September 11, 2011 and U.S. justifications for military force in Afghanistan against the Taliban regime, see Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 CHI. J. INT'L L. 83 (2003).

[44] Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 38, ch. II, cmt. 2, at 39.

organs should be considered those of the state and under which circumstances.[45]

Article 8 is the most relevant article with regard to non-state actors and state responsibility: "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[46] The degree of control exercised by a state has been a key issue in a number of international cases. This includes the *Military and Paramilitary Activities in and Against Nicaragua* case in the International Court of Justice, which established that "effective control" of non-state actors was needed to attribute state responsibility to the actions of those organizations. Under "effective control," for the United States to have responsibility for the international violations of the contras in Nicaragua, it would have had to have "directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State [Nicaragua]."[47] This contrasts with the standard of "overall control" in the International Criminal Tribunal for the Former Yugoslavia case *Tadic*.[48] The Appeals Chamber in that case concluded each case depends on the specific facts of a particular circumstance and that the standard of "overall control" goes beyond financing and equipping and includes "participation in the planning and supervision of military operations."[49]

---

[45] Article 4 states that the conduct of the organ of a state can be legislative, executive or judicial, whatever its position or function in the central Government; Article 5 addresses "conduct of persons or entit[ies] . . . exercis[ing] elements of governmental authority"; Article 6 considers "conduct of organs placed at the disposal of a State by another State"; and Article 7 states that the conduct of an organ or person acting under governmental authority may be attributed to the state, even if that organ or individual is "exceed[ing] its authorities or [contravening] instructions." *Id.*, ch. II, cmt. 8, at 39.

[46] *Id.*, art. 8, at 47.

[47] Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, 64 (June 27).

[48] Prosecutor v. Tadic, Case No. IT-94-1-A, Judgement, ¶ 121 (July 15, 1999).

[49] Tadic, ¶ 145. The Tadic standard is a lower threshold to cross than the Nicaragua standard, although the actions of the United States in attributing responsibility for the actions of al Qaeda to the Taliban regime in Afghanistan is still a different threshold. The United States argued that the Taliban was complicit in al Qaeda's actions because it did not prevent the organization from using Afghanistan as a planning and operations base. *See* Jinks, *supra* note 43.

Thus, the scope of the *ILC Draft Articles* is generally limited to state-to-state issues, although it does allow for attributing state responsibility for unlawful actions by non-state actors to the state. However, there must be a demonstration of instruction, direction, or control in order to attribute such conduct to the state. As is clarified in the commentaries, the actions of a state-owned and controlled corporation are generally not attributable to the state, unless the entity is a "corporate veil" for illegal actions of the state.[50] Therefore, whether a state may assume responsibility for non-state conduct depends greatly on the facts of each case and must be based on whether the non-state group is instructed, directed, or controlled by the state or any of its organs.

2. APPLICABILITY OF ILC DRAFT ARTICLES TO CYBER

In order for a state to be held responsible for a non-state group's activities in cyberspace, based on the principles set forth in the ILC Draft Articles, two criteria must be met. First, the action must be a violation of a primary obligation of the state. Second, if a non-state actor takes the action, the state must have either instructed, directed, or controlled the group's action.

The *ILC Draft Articles* may accordingly be useful in holding a nation responsible for malicious attack traffic that originated in or merely transited its networks, but only in the unlikely case this could be considered a violation of "primary obligation" of states. Using another example, under the ILC Draft Articles, Estonia would have had to establish that the activity breached a primary obligation of Russia and that the actions were instructed, controlled, or directed by an organ of the state.

While it is possible to imagine a situation in which malicious cyber activity would constitute violations of primary obligations, what the world has seen to date would not reach those thresholds. Therefore, the other principles discussed below, and primarily the principle of transboundary harm, might be more helpful in dealing with non-state actors.

---

[50] Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 38, art. 8, cmt. 6, at 48.

3. THE CUSTOMARY NORM OF GOOD NEIGHBORLINESS

The customary norm of good neighborliness is also potentially applicable to cyberspace. The custom is generally considered to be a product of international environmental law, including the *Trail Smelter* case discussed in detail below. The principle will be discussed in a broader context, as it encompasses the tension between obligation and sovereignty, both of which have considerable implications for cyberspace. While the principle has grounding in some other capacities, the principle is in essence a norm of international environmental law.[51] For international environmental law, good neighborliness is considered a general principle that dictates that states utilize their resources in a way that will not damage the environment, particularly that of their neighbors. Additionally, if a breach of the principle of good neighborliness is a breach of a primary obligation and one applies this environmental principle to cyberspace, the *ILC Draft Articles* may have more applicability in that context.

The principle of good neighborliness establishes that "no state is entitled to use its land in a way that might infringe on the rights of another nation."[52] This norm is further solidified in *Trail Smelter*, demonstrating that the presence of good neighborliness in both an international arbitration and as a general principle adds extra weight to state responsibility and liability to prevent unlawful or harmful transboundary activity to negatively affect another state. The *Trail Smelter* arbitration discussed below also helped to establish the customary status of a principle of "good neighborliness" between nations,[53] which is further developed through its gradual adoption reflected in other international instruments, including the *Stockholm Declaration*.

Good neighborliness was addressed, for example, in the Co-operation in the Field of the Environment Concerning Natural

---

[51] For good neighborliness in other contexts, see, for example, Treaty of Good-Neighborliness and Friendly Cooperation, P.R.C.-Russ., July 24, 2001, Ministry of Foreign Affairs of the People's Republic of China, *available at* http://www.fmprc.gov.cn/eng/wjdt/2649/t15771.htm.

[52] Mark S. Blodgett et al., *A Primer on International Environmental Law: Sustainability as a Principle of International Law and Custom*, 15 ILSA J. INT'L & COMP. L. 15, 21 (2008).

[53] Geoffrey Palmer, *New Ways to Make International Environmental Law*, 86 AM. J. INT'L L. 259, 265 (1992).

Resources Shared by Two or More States (UNEP Draft Principles).[54] The 1978 UNEP Draft Principles were written pursuant to a request by the U.N. General Assembly and were released two years after the Working Group began its examination of the topic. When the General Assembly requested the review, it made clear that any results from the Working Group would be considered only principles and not binding international law.[55] Principle 7 of the UNEP Draft Principles states:

> Exchange of information, notification, consultations and other forms of co-operation regarding shared natural resources are carried out on the basis of the principle of good faith and in the spirit of good neighborliness and in such a way as to avoid any unreasonable delays either in the forms of co-operation or in carrying out development or conservation projects.[56]

Although the UNEP Draft Principles, like the ILC Draft Articles, do not create international law, they reaffirm good neighborliness and its obligations as a rule of international law.[57] While this norm clearly applies to environmental issues, including conservation, it is possible to apply the same concepts and intentions of the UNEP Draft Principles to cyberspace.

An additional aspect of good neighborliness is the "duty to cooperate in investigating, identifying, and avoiding environmental harm."[58] Further, this norm can incorporate the exchange of general

---

[54] U.N. Env't Program, Governing Council Approval of the Report of the Intergovernmental Working Group of Experts on Natural Resources Shared by Two or More States: Co-operation in the Field of the Environment Concerning Natural Resources Shared by Two or More States, U.N. Doc. GC.6/CRP.2, reprinted in 17 I.L.M. 1091 (1978) [hereinafter UNEP Draft Principles].

[55] PHILIPPE SANDS, PRINCIPLES OF INTERNATIONAL ENVIRONMENTAL LAW 43–44 (2d ed. 2003).

[56] UNEP Draft Principles, *supra* note 54, at 1099.

[57] Additionally, while good neighborliness is a foundational customary principle in international environmental law, scholars emphasize that it is not a jus cogens norm, nor could it ever reach that status. *See* Eva M. Kornicker Uhlmann, *State Community Interests, Jus Cogens and Protection of the Global Environment: Developing Criteria for Peremptory Norms*, 11 GEO. INT'L ENVTL. L. REV. 101 (1998).

[58] Max Valverde Soto, *General Principles of International Environmental Law*, 3 ILSA J. INT'L & COMP. L. 193, 197 (1996).

information and prior notification.[59] While prior notification should be provided when possible, a state should also notify relevant states of an emergency or event that will have transboundary effects.[60] While good neighborliness does not require that a state consulting with other states be bound by their opinions, consultation and notification are crucial aspects of good neighborliness.

The scope of this norm may be limited in that it applies to responsibilities owed by states to states, but the activity in question need not be the action of a state. Rather, this norm requires that a state notify and consult whenever activities within its boundaries will have a negative impact on the territories or environment of another state. Consider, for instance, the obligations of the Soviet Union to notify states of the nuclear disaster at Chernobyl as the event was happening and to pay damages later.[61] However, the Chernobyl accident also illustrates the limitation of recovering damages and enforcing decisions.[62] In terms of enforcing this rule, it seems as if the norm has limited applicability because of its position as a general principle—there is simply relatively little to build up scope and enforceability.

A state's remedial options for a violation of good neighborliness are the same as for other disputes, including the traditional levers of

---

[59] *Id.* at 198; *see also* U.N. Conference on Environment and Development, Rio de Janiero, Braz., June 3–14, 1992, Rio Declaration on Environment and Development, U.N. Doc. A/CONF.151/5/Rev.1 (1992), reprinted in 31 I.L.M. 876, 879 (1992) [hereinafter Rio Declaration].

[60] Soto, *supra* note 58, at 198–99; Rio Declaration, *supra* note 59, at 879.

[61] *See* Linda A. Malone, *The Chernobyl Accident: A Case Study in International Law Regulating State Responsibility for Transboundary Nuclear Pollution*, 12 COLUM. J. ENVTL. L. 203, 207 n. 43 (1987).

[62] As Malone states, "potential and actual litigants soon discovered that although the Soviet Union was certainly responsible for damage from the accident under international law recovery was uncertain and enforcement virtually impossible." *Id.* at 207. It was difficult for victims of Chernobyl to receive benefits from the Soviet Union after the disaster, an issue that continues, particularly regarding long-term health care and benefits from the Government of Russia. *See*, e.g., Mareike Aden, *The Legacy of Chernobyl Continues to Shape Victims' Lives*, DEUTSCHE WELLE (Apr. 25, 2011), http://www.dw-world.de/dw/article/0,,15028249,00.html; Alastair Fee, Chernobyl Victims Struggle with Consequences of Radiation Exposure, U.S. NEWS & WORLD REP., Apr. 24, 2008, http://www.usnews.com/news/world/articles/2008/04/24/chernobyl-victims-struggle-with-consequences-of-radiation-exposure; Press Release, Int'l Atomic Energy Agency, Chernobyl: The True Scale of the Accident (Sept. 5, 2005), http://www.iaea.org/newscenter/pressreleases/2005/prn200512.html.

statecraft and perhaps the International Court of Justice if the consequences are sufficiently severe. However, it is the particulars of the case that dictate the applicability of these international norms. This is why it is important for states to clarify expectations when applying these norms to cyberspace. If one considers botnets as a kind of transboundary emission or significant form of transboundary harm, the complaining state must be able to demonstrate damage in violation of the principle of good neighborliness. Therefore, it is not an issue of demonstrating that such botnets exist, but rather the extent of damage caused by them. This, once again, demonstrates the need to have a spectrum of state responsibility so that the issue of technical attribution does not sidetrack states. The principle of good neighborliness demonstrates that while harm must be demonstrated, identifying the exact user of the computer controlling a command and control server is not necessary when extending the metaphor to cyberspace. The complexities of technical attribution need not therefore delay the pursuit of a remedy. Rather, a state must request through traditional political and diplomatic channels that the state address the issue of transboundary harm emanating from its territory.

4. APPLICATION OF GOOD NEIGHBORLINESS TO CYBER

As applied to cyberspace, the principle of good neighborliness would dictate that a state has an obligation to limit the negative impacts of actors in its territory from negatively affecting the territory or interests of another state. Using the language in the UNEP Draft Principles, the "shared natural resources" in question can be the interconnected networks of cyberspace because something in one country's networks can easily and quickly have negative consequences in the networks of other states. To that extent, using the principle of good neighborliness, a state should exchange information, notify others of potential issues, and consult with other states on malicious activity in cyberspace. The goal of such information sharing and obligations would be to improve cooperation against combating clearly malicious activities, including botnets, DDoS attacks, and other mechanisms that cause havoc in cyberspace. Such an obligation in environmental law is expanded upon in Trail Smelter, which provides context for how such an obligation would function vis-à-vis cyberspace.

C. THE FINDING OF STATE LIABILITY IN TRAIL SMELTER

The Trail Smelter arbitration case is a foundational environmental case, but also has broad implications beyond international environmental law. The case has implications for state sovereignty and sets a key precedent in delineating the responsibilities of states for incidents that cause transboundary harm, even if a non-state actor causes such harm.[63] In the Trail Smelter arbitration case, the United States and Canada entered into arbitration to resolve a dispute about sulfur dioxide emissions from a Canadian smelting plant that were traveling over the border into U.S. jurisdiction. In order to avoid polluting the area directly surrounding the plant and to accommodate increased production, the Canadian smelter company had built a 409-foot smokestack in 1925, which in turn sent the plant's fumes "higher into the wind stream and therefore further down the valley."[64] The fumes were thus causing increased pollution in Washington state, leading farmers to complain of "irreparable damage" to their crops, grazing lands, and orchards.[65] The ensuing dispute lasted over fifteen years, with the first Tribunal held in 1937. The 1941 final report attributed responsibility to the smelting company and to Canada, which voluntarily took on the liability in this circumstance.[66]

While the actors in the initial dispute were private actors, the arbitration shifted the matter into a public settlement between two states. In its final report, the Trail Smelter Tribunal concluded:

> [U]nder the principles of international law . . . no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and

---

[63] Austen L. Parrish, Sovereignty's Continuing Importance: Traces of Trail Smelter in the International Law Governing Hazardous Waste Transport, *in* TRANSBOUNDARY HARM IN INTERNATIONAL LAW: LESSONS FROM THE TRAIL SMELTER ARBITRATION 181 (Rebecca M. Bratspies & Russell A. Miller eds., 2006).

[64] James R. Allum, "An Outcrop of Hell": History, Environment, and the Politics of the Trail Smelter Dispute, *in* TRANSBOUNDARY HARM IN INTERNATIONAL LAW: LESSONS FROM THE TRAIL SMELTER ARBITRATION 13, 15 (Rebecca M. Bratspies & Russell A. Miller eds., 2006).

[65] *Id.*

[66] Trail Smelter (U.S. v. Can.), 3 R. Int'l Arb. Awards 1905 (1938 & 1941).

> the injury is established by clear and convincing evidence.[67]

The above statement is often cited as an important declaration of state responsibility for transboundary environmental harm. Still, the statement includes a number of caveats and limits to the range of state responsibility involved. First, the holding in this report refers to responsibility for a specific incident for which cause and effect were readily identifiable. Responsibility for general environmental damage with diffuse causes is not discussed. Second, state responsibility applies when "the case is of serious consequence," and only when there is manifest injury "established by clear and convincing evidence."[68] These are important limitations to the scope of state responsibility. Although the arbitration was not binding, it established certain state obligations for transboundary harm and the principle further elucidated in Trail Smelter has developed into customary law that has crystallized over the ensuing decades.[69] Additionally, Trail Smelter adds weight to the norm of good neighborliness discussed above.

1. APPLYING TRAIL SMELTER TO CYBER

According to the findings of the Tribunal, the principle of Trail Smelter would seem to apply to the cyber equivalent of transboundary harm if it were of "serious consequence" and "established by clear and convincing evidence." Still, what constitutes "serious consequence" can be difficult to ascertain and is particular to the circumstances of a specific incident. However, it seems clear that the cyber attacks against Estonia would exemplify a case of "serious consequence" because the majority of banking, e-commerce, government, and media

---

[67] *Id.* at 1965.

[68] *Id.*

[69] Legal scholars also note that despite the impressive reputation of the Tribunal decision, the procedure of the case has never been repeated. Although the procedure and the format of the decision places caveats on the scope of the decision, the Trail Smelter arbitration and the subsequent history still clearly establishes customary international law regarding state responsibility and liability. *See* John H. Knox, The Flawed Trail Smelter Procedure: The Wrong Tribunal, the Wrong Parties, and the Wrong Law, *in* TRANSBOUNDARY HARM IN INTERNATIONAL LAW: LESSONS FROM THE TRAIL SMELTER ARBITRATION 66 (Rebecca M. Bratspies & Russell A. Miller eds., 2006).

websites and services were forced offline for weeks in a country heavily dependent on e-services for all sectors of society.

Even absent such a massive attack, it is likely that "serious consequence" could still be found. Botnets are responsible for millions of dollars in damages through theft of personal information, sending spam, and DDoS attacks. A nation may clearly have a claim against another nation that continually allowed botnets to operate from its territory.

The requirement of "clear and convincing evidence" need not be insurmountable. While the ultimate author of an attack, such as against Estonia, may not be known (or provable), the geographic location of particular botnet computers and their automated controllers is generally well understood. Trail Smelter establishes state responsibility for actions of private actors in a single nation that nonetheless have international implications. Many computer network attacks and computer network exploitation schemes take just this form.

The burden on a target state to establish another state's responsibility might be greater if it were alleged that the defendant state had instigated or supported an attack, as opposed to being insufficiently vigilant in preventing activity or passively allowing activities that the defendant state had an obligation to prevent. In this case, Trail Smelter would be less useful than one of the other norms listed in this article.

Trail Smelter is also helpful in determining the role of compensation once transboundary harm has occurred. The "polluter pays" principle outlines when the polluter bears the responsibility for paying for any prevention and cleanup measures, as well as any damages.[70] However, as one scholar points out, the private company in Trail Smelter was not a party to the arbitration. A more accurate statement of the principle would seem to be the "polluter's nation pays."[71] In other words, for compensation and liability to be imposed based on principles established through good neighborliness and Trail Smelter, which are also solidified in the ILC Draft Articles, there must be direct responsibility of the state.[72] At the same time, using the

---

[70] Mark Anderson, Derivative Versus Direct Liability as a Basis for State Liability for Transboundary Harms, *in* TRANSBOUNDARY HARM IN INTERNATIONAL LAW: LESSONS FROM THE TRAIL SMELTER ARBITRATION 99, 99 (Rebecca M. Bratspies & Russell A. Miller eds., 2006).

[71] *See id.*

[72] *Id.*

proposed "spectrum of state responsibility,"[73] a state could still be considered responsible for a large range of malicious cyber activity using the international environmental norms discussed, but would potentially not have to pay damages for the harm inflicted by either the state or a non-state actor within its jurisdiction.

D. PRINCIPLE 21 OF THE STOCKHOLM DECLARATION

State liability and responsibility in international environmental policy became further entrenched with the first environmental conference in Sweden in 1972.[74] This conference, the United Nations Conference on the Human Environment, produced the Stockholm Declaration.[75] The most relevant principle within the Stockholm Declaration is Principle 21:

> States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own resources pursuant to their own environmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction.[76]

This text is a codification of the custom established in the Trail Smelter arbitration and is considered by some to be the "progeny" of the Trail Smelter decision.[77] While the Stockholm Declaration is an

---

[73] *See* Jason Healey, *Beyond Attribution: A Vocabulary for National Responsibility for Cyber Attacks*, 18 BROWN J. WORLD AFF. (forthcoming 2011).

[74] The Stockholm Conference was not the first environmental conference, nor was the Stockholm Declaration the first international treaty. Earlier environmental conferences include the 1968 African Convention on Conservation of Nature and Natural Resources and the 1971 Ramsar Treaty. LOUKA, *supra* note 42, at 30.

[75] U.N. Conference on the Human Environment, Stockholm, Swed., June 5–16, 1972, Declaration of the United Nations Conference in the Human Environment, U.N. Doc. A/CONF.48/14 and Corr. 1 (1972), reprinted in 11 I.L.M. 1416 (1972) [hereinafter Stockholm Declaration].

[76] *Id.* at Principle 21.

[77] Stephen C. McCaffrey, Of Paradoxes, Precedents, and Progeny: The Trail Smelter Arbitration 65 Years Later, *in* TRANSBOUNDARY HARM IN INTERNATIONAL LAW: LESSONS

important step forward in international environmental law, Principle 21 does not provide additional clarity as to the exact scope of state responsibility. The balancing of sovereign rights and the responsibility to other states has created much debate even in the wake of the Stockholm Declaration and is also reflected in the continuing dialogue about the role of the state and sovereignty in cyberspace.

Principle 21 is generally a state-to-state obligation, but it does further establish state responsibility for the actions of non-state actors using state territory or resources. The state's obligation to "ensure that activities within [a State's] jurisdiction or control" do not damage the environment of others implicates an obligation regardless of the actor's responsibility for the initial activities.[78] The state, therefore, has the obligation to effectively govern and regulate its own resources. While still a state-level obligation, this also addresses obligations for non-state activities. Still, the consequences of a violation of the Stockholm Declaration are limited. The Stockholm Declaration is not binding upon states, although some articles are seen as codification of customary international law. Because of the nature of the Stockholm Declaration, it has limited enforcement, although it can be cited as a clear articulation of an international norm should a state authorize, passively permit, or fail to stop its territory from being used in a manner contrary to the rights of other states.

In referring, however, both to states' "sovereign right to exploit their own resources" and their "responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other states," Principle 21 seems to give equal weight to both concepts of sovereignty and international obligation in the context of environmental protection.[79] The tension in Principle 21 is also found in Trail Smelter, although it is a further codification of the rights and obligations of a state.

1. APPLICATION OF PRINCIPLE 21 TO CYBER

As applied to cyberspace, the "sovereign right to exploit their own resources,"[80] may permit certain rights within a nation's networks;

FROM THE TRAIL SMELTER ARBITRATION 34, 41 (Rebecca M. Bratspies & Russell A. Miller eds., 2006).

[78] Stockholm Declaration, *supra* note 75, at Principle 21.

[79] *Id.*

[80] *Id.*

however, once those internal actions affect networks outside of a state's networks and cyberspace, the state may have an obligation to ensure that such activity does not cause significant damage to the networks and users of the broader Internet. This can include DDoS attacks or the use of botnets.

Using the example of Estonia, applying the norms behind Principle 21 would require that if Russia—or indeed any other country—was aware of non-state actors using its networks to "herd" botnets or launch DDoS attacks, it would have an obligation to prevent that "transboundary harm" or "damage" afflicting Estonia. If the DDoS attacks were primarily targeting and affecting domestic websites and services, Russia would not have this obligation. However, once the attacks targeted external networks, sites, and services, under Principle 21, Russia would have had at least a political obligation to address and mitigate these attacks once they reached a certain level of scope, severity, and intensity, similar to the Pictet factors discussed above. Determining whether the circumstance reaches those thresholds will depend on the specific facts, as do all major incidents or controversies in international law and international politics. Therefore, applying Principle 21 to cyberspace, while needing political endorsement, would not be significantly different than other issues in the international system.

While a potentially fruitful avenue to pursue, the analogy is not without its difficulties. Networks are not obviously "natural resources," as stated in Principle 21, though a convincing case might be made that they should be treated "as if" they were. Additionally, while jurisdiction and sovereignty are manifested differently in cyberspace, these two concepts still apply and may actually prove problematic for an open cyberspace. If the zone of sovereignty embodied in the first half of Principle 21 applies to cyberspace, it could be invoked to further justify harsh Internet censorship, counter to key U.S. and Western values of free speech and freedom on information.

E. THE IMPOSITION OF STATE RESPONSIBILITY IN CORFU CHANNEL

Lastly, Corfu Channel establishes state responsibility for an omission of an action. While the facts of the case are not about environmental damage, the norm established is relevant for transboundary harm and damage to the territory and jurisdiction of another state. This case concerns two incidents in 1946 when an international court held Albania responsible for mines in its waters,

two of which damaged British destroyers.[81] Even though Albania objected that it had not placed the mines in the Strait, the Court decided that Albania had the responsibility to notify other states of the minefield and to warn the British ships of the imminent danger to which the minefield exposed them.[82] The Court held:

> [Albania's obligations are based] . . . on certain general and well-recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war; the principle of the freedom of maritime communication; and every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.[83]

Although not an environmental law case per se, Corfu Channel is important because its holding has been repeated in pollution and hazardous activities cases involving activities within one state that have adverse affects on other states, creating, for example, the duty to notify of pollution.[84] Simply put, Corfu Channel establishes that if a state knows or should have known about an activity, it has an obligation to either mitigate the consequences or, if possible, notify the other state before the activity occurs.

This norm is a state-to-state obligation, but again it determines that a state can be responsible for "knowingly [allowing] its territory to be used for acts contrary to the rights of other States." The enforceability of this norm is dependent on the way in which a "victim" state would address the violation. If the case was significant enough to reach the International Court of Justice, Corfu Channel is a firm statement of a state's obligation to other states. Because the norm is not enshrined in treaty law, there is no obvious enforcement mechanism, but states may pursue remedies as they would for other violations of international law and custom. This issue of remedy and enforceability is not unique to applying Corfu Channel to cyberspace.

---

[81] Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4 (Apr. 9).

[82] LOUKA, *supra* note 42, at 39.

[83] Corfu Channel, *supra* note 81, at 22 (emphasis added).

[84] LOUKA, *supra* note 42.The ILC Draft Articles also cite Corfu Channel as an example of when an omission of the state can still invoke that state's responsibility to prevent the breach of the primary obligation. Draft Articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 38, ch. IV, cmt. 4, at 64.

In fact, it is this issue of enforceability and remedy that may be the most important for using these norms and principles in an international political context rather than an international legal context.

Generally, the norm further established in Corfu Channel requires that when states are aware of activities that will impede the rights of other states, the initial state has the obligation to prevent the activities.

1. APPLICATION OF CORFU CHANNEL TO CYBER

As applied to cyberspace and the Estonian incident, if Russia was aware that actors in its territory were responsible for the attacks against Estonia, it would have had an obligation to prevent those acts. Again, it is a question of thresholds and whether such activity rises to the level of damage in both the Trail Smelter and Corfu Channel cases. However, in the case of Estonia, in which many sectors were crippled for weeks on end, it seems the attacks could be characterized as transboundary harm. Because the attacks against Estonia did not rise to the level for the application of the laws of armed conflict, it may be more applicable to use norms developed in international environmental law in cases such as Estonia to curtail similar incidents and address the diplomatic implications should similar incidents occur.

Similarly, for many years the United States has been one of the main sources of malicious software and botnets. It is conceivable that the Corfu Channel decision might be used against the United States government, which seems to be obligated to prevent these attacks when they impede the rights of other states.

IV. ANALYSIS AND CONCLUSION

Although the judgments and agreements discussed above often arose in the context of environmental protection, they engage the tension more generally between state sovereignty and a state's obligations to others. This friction is apparent in inter-state relations and non-state actors' activities in cyberspace. While it is not always easy to identify and stop "cyber pollution," it is possible to both stop malicious activity (once it is identified as such) and to disable botnets and sources of malicious software. Recent takedowns of the Rustock and Waledac botnets show how international coordination between

states and non-states can effectively stop malicious activities.[85] And although these were addressed through a criminal approach, they are examples of how environmental norms may be useful to motivate and shame complicit or passive states into stopping malicious activity in cyberspace. At the very least, a state intentionally ignoring non-state actors who are causing damage to other states should be held accountable, especially when one considers the precedent set in Corfu Channel.

Overall, the international environmental legal framework can be useful in attributing state responsibility and liability for computer network attacks against another state. The application of key norms in international environmental law can push forward development of international law in cyberspace because it takes away some of the "newness" of the problem. Certainly, there will be aspects of cyberspace that will require different kinds of norms and new regulations and expectations for state behavior. However, there are times where existing frameworks with strong legal roots can contextualize problems, making them less daunting. As Dupuy and Hoss conclude, "The existence of an appropriate legal regime to deal with such issues . . . puts into question the many and varied attempts to create new laws to deal with new problems."[86] While cyber-specific international law may be lacking, the international legal regime can provide guidance, as many of the "new" cyber issues are actually similar to those in the "kinetic" world. Accordingly, a return to foundational principles of international law can improve the governance and regulations of cyberspace.

Key international environmental norms are applicable to the actions of states and non-state actors in cyberspace because transboundary harms in cyberspace pose analogous problems of balancing sovereignty and international obligation. These norms may be able to resolve the tension between sovereignty and obligations to

---

[85] *See* Posting of Richard Boscovich to Microsoft on the Issues blog, Taking Down Botnets: Microsoft and the Rustock Botnet, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/18/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx (Mar. 17, 2011, 6:36 PM); Posting of Tim Cranton to Microsoft on the Issues blog, What We Know (and Learned) from the Takedown of the Waledac Botnet, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/03/16/what-we-know-and-learned-from-the-takedown-of-the-waledac-botnet.aspx (Mar. 16, 2010, 11:51 AM).

[86] Pierre-Marie Dupuy & Cristina Hoss, Trail Smelter and Terrorism: International Mechanisms to Combat Transboundary Harm, *in* TRANSBOUNDARY HARM IN INTERNATIONAL LAW: LESSONS FROM THE TRAIL SMELTER ARBITRATION 225, 239 (Rebecca M. Bratspies & Russell A. Miller eds., 2006).

other international actors. The problems of cyberspace are large in number and in complexity. However, other international legal problems have been vast and complicated and have still been addressed by international law with success. The complexity of a problem should not necessarily preclude the application of international law, nor should it require a completely new international legal framework.

The scope of international environmental legal norms is helpful in addressing a range of activities that cover state responsibility for the actions of private actors within a state's jurisdiction that have significant impact upon the territory of another state. As applied to cyberspace, this could develop into a norm in which states are obligated to ensure that the networks under their jurisdiction are not used contrary to the rights of other states, including an obligation to combat of DDoS, botnets, and other clearly malicious activity. Again, this is not an issue of policing content, but rather of preventing the most indefensible, malicious developments in cyberspace. The enforceability of these norms is difficult, but not in any manner significantly different than other issues in international law. Similarly, the issue of remedy is limited based on enforceability and states must rely on the traditional tools of statecraft, diplomacy, and military force when necessary to address violations of international law. While this is not specific to cyber issues, it should in some way be reassuring as these are the tools used in international politics and diplomacy and they have been used for centuries.

Still, while these norms seem to have compatible applicability to cyberspace, states remain the international actors who need to push forward the dialogue on this issue and consent to be bound by these norms in the sphere of cyberspace. International environmental norms offer a constructive example of balancing sovereignty with due diligence and obligations to other nations. States should therefore continue engagement in international forums. Dialogue and the discussion of definitional matters should ideally be established before the international system sees either a further proliferation or increase in severity of cyber attacks. While international law struggles with creating frameworks preventatively, states should still commit themselves to continued dialogue in order to reach consensus on appropriate state and non-state behavior in cyberspace. It is this issue that demonstrates the value in pursuing norms first as a political issue

followed by a potential legal issue depending on the maturation of the norm.[87]

International environmental law is an under-utilized framework for addressing problems in cyberspace that do not fall under the framework of armed conflict or are not strictly criminal in nature. Because this makes up much of current cyber conflict, there is great utility in deriving principles from international environmental law. Other international law frameworks have been proposed for cyberspace, but environmental legal norms may also provide solutions to the current and emerging issues in cyber security, cyber conflict, and cyber defense. State responsibility is a crucial underpinning for international environmental law and can also serve as an important foundation for future expected norms and behaviors within cyberspace.

[87] Examples of organizations that may be good frameworks for this dialogue include the U.N. Group of Governmental Experts, Organization for Economic Co-operation and Development (OECD), or G-20. Regionally, organizations like the Organization of American States (OAS) and the Asia-Pacific Economic Cooperation (APEC) could provide neutral frameworks for discussion on norms and cyber policy as well.